WHAT IS CLAIMED IS:

1. A token adapted to provide access to an account, the token comprising:

a memory configured to store an image of a biometric.

2. The token of Claim 1 wherein said memory is an integrated circuit configured to store the image of the biometric.

3. The token of Claim 2 wherein said biometric image is a finger print image stored in the memory in one of Tiff, JPEG and bitmap formats.

4. The token of Claim 3 further comprising:

a magnetic stripe adapted to store data related to the account.

5. The token of Claim 4 wherein said token is a card.

6. The token of Claim 5 wherein said card is formed from material selected from a group consisting of plastic and metal.

7. A system adapted to receive a token, said token comprising an integrated circuit memory configured to store an image of a biometric, said token adapted to provide access to an account, said system comprising:

a processor configured to read the biometric image stored in the integrated circuit memory disposed in the token.

8. The system of Claim 7 wherein said processor is further configured to generate a binary number from the stored image of the biometric and in accordance with a preselected algorithm.

9 . The system of Claim 8 further comprising a biometric sampler adapted to sample and capture an image of at least one biometric of the token holder at the location in which the system is stationed.

10. The system of Claim 9 wherein said processor is further configured to generate a second binary number from the at least one biometric image of the token holder sampled and captured at the location in which the system is stationed, wherein said second binary number is generated in accordance with the preselected algorithm.

11. The system of claim 10 wherein said processor is further configured to compare the first and second binary numbers to determine whether they match within a predefined tolerance limit.

12. The system of 11 wherein said processor is further configured to generate a third binary number from one of the first and second binary numbers if the first and second binary numbers match each other within the predefined tolerance limit, wherein said third binary number is generated in accordance with a second preselected algorithm.

13. The system of claim 12 wherein said third binary number has fewer bits than either of the first and second binary numbers.

14. The system of Claim 13 further comprising a second processor configured to receive the third binary number from the first processor.

15. The system of Claim 14 wherein said first and second processors are located at different sites.

16. The system of Claim 15 wherein said second processor receives the third binary number from the first processor via wired or wireless communication lines.

17. The system of Claim 16 wherein said second processor is coupled to a database which maintains a fourth binary number extracted from a same biometric image source from which the biometric image stored in the memory is supplied, wherein said fourth binary number is extracted in accordance with the second preselected algorithm.

18. The system of Claim 17 wherein said second processor is configured to retrieve the fourth binary number from the database and compare the retrieved fourth binary number to the third binary number it receives from the first processor to determine whether a match exists between the third and fourth binary numbers within a second predefined tolerance limit.

19. The system of Claim 18 wherein if the second processor determines that a match exists between the third and fourth binary numbers then access to the account associated with the token is granted.

20. The system of Claim 19 wherein if the first processor determines that the first and second binary numbers do not match each other within the first predefined tolerance limit then access to the account associated with the token is denied.

21. The system of Claim 20 wherein if the second processor determines that the third and fourth binary numbers do not match each other within a second predefined tolerance limit then access to the account associated with the token is denied.

22. The system of Claim 21 wherein the second processor further receives information related to the account with which the token is associated with from the first processor.

23. The system of Claim 22 further comprising:

a key pad configured to enable the token holder to enter information related to the account into the system; and

a display configured to display messages to the token holder.

24. The system of Claim 23 further comprising:

a magnetic read device adapted to receive information stored on a magnetic medium disposed on the token.

25. The system of Claim 24 wherein the at least one biometric sample is a finger print sample and wherein the image of the at least one biometric sample of the token holder sampled and captured by the biometric sampler is formatted according to one of Tiff, bitmap and JPEG image format standards.

26. A method of forming a token adapted to provide access to an account, the method comprising:

forming a memory;

storing an image of a biometric in the memory; and

disposing the memory on the token.

27. The method of Claim 26 wherein said memory is an integrated circuit memory configured to store the image of the biometric.

28. The method of Claim 27 wherein said biometric image is a finger print image.

29. The method of Claim 28 wherein said finger print image is stored in the memory in one of Tiff, bitmap and JPEG formats.

30. The method of Claim 29 further comprising:

disposing a magnetic stripe adapted to store data related to the account on the token.

31. The method of Claim 30 wherein said token is a card.

32. The method of Claim 31 wherein said card is formed from material selected from a group consisting of plastic and metal.

33. A method of authorizing access to an account with a token, the method comprising:

receiving the token on which a memory configured to store an image of a biometric is disposed; and

reading the biometric image stored in the memory disposed on the token.

34. The method of Claim 33 further comprising:

generating a binary number from the biometric image stored in the memory in accordance with a preselected algorithm.

35. The method of Claim 34 further comprising:

capturing at least one biometric image of the token holder at the location in which access to the account associated with the token is requested.

36. The method of claim 35 further comprising:

generating a second binary number from the at least one biometric image captured from the token holder in accordance with the preselected algorithm.

37. The method of claim 36 further comprising:

comparing the first and second binary numbers to determine whether they match within a predefined tolerance limit.

38. The method of claim 36 further comprising:

extracting a third binary number from one of the first and second binary numbers if the first and second binary numbers match each other within the predefined tolerance limit, wherein said third binary number is extracted in accordance with a second preselected algorithm.

39. The method of Claim 38 wherein said third binary number has fewer bits than the first and second binary numbers.

40. The method of Claim 39 further comprising transmitting the third binary number to another location via wired or wireless communication lines.

41. The method of Claim 40 further comprising:

comparing the transmitted third binary number to a fourth binary number maintained in a database to determine whether a match exists between the third and fourth binary numbers within a second predefined tolerance limit, wherein said fourth binary number is extracted from a same biometric image source from which the biometric image stored in the memory is supplied, wherein said fourth binary number is extracted in accordance with the second preselected algorithm; and

granting access to the account associated with the token if the third and fourth binary numbers match within a second predefined tolerance limit.

42. The method of Claim 41 further comprising:

denying access to the account associated with the token if the third and fourth binary numbers do not match within the second predefined tolerance limit.

43. The method of Claim 42 further comprising:

transmitting account related information via the wired or the wireless communication lines, wherein the account related information are retrieved from the token.

44. The method of Claim 43 further comprising:

receiving information related to the account from the token holder; and

displaying messages related to the account to the token holder.

45. The method of Claim 43 further comprising:

storing account related information on a magnetic stripe disposed on the token.

46. The method of Claim 45 wherein biometric image is stored in the memory according to one of Tiff, bitmap and JPEG image format standards.

47. The method of Claim 46 wherein said biometric is a finger print.

48. The method of Claim 47 wherein said memory is an integrated circuit memory.